ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Servicios ***Fast Review*** de **Ciberseguridad** para **PYMEs**

RETOS

Las PYMEs se enfrentan a una serie de complejos desafíos, azuzados por un mercado tremendamente ágil y en constante evolución. Desde la incertidumbre económica hasta la competencia feroz, las PYMEs deben adaptarse a las cambiantes tendencias y a la rápida evolución de la tecnología, manteniéndose actualizadas y flexibles para garantizar la relevancia de sus productos y servicios. La digitalización también está poniendo de manifiesto el crecimiento de la superficie de ataque, aumentando así las posibilidades de sufrir un ciberincidente con las consecuencias que ello puede conllevar para su supervivencia.

CIFRAS CLAVE

- El **83%** de las **PYMEs no están preparadas** para responder ante un **ciberataque**.
- El **30%** de las **PYMEs** teme al **phishing** como una de sus principales **ciberamenazas**.
- El **91%** de las **PYMEs** aún no cuenta con un **ciberseguro de responsabilidad.**

SOLUCIONES

Conocemos profundamente las necesidades de las PYMEs, y tratamos de darles cumplimiento diseñando, implantando, manteniendo y operando planes integrales de seguridad basados en las seis funciones del NIST (Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación). Dentro de ellas, nuestro servicio *Fast Review* permite conocer, en tan solo una semana, el estado real de la compañía a nivel de ciberseguridad. Este servicio se encuentra dirigido a PYMEs de menos de 50 empleados.

Día 1: Reconocimiento del entorno.
Revisamos el estado global de la ciberseguridad mediante chequeo del cumplimiento de los controles prioritarios de la matriz CIS:

a. Inventario de dispositivos autorizados y no autorizados.
b. Inventario de software autorizado y no autorizado.
c. Configuraciones seguras en equipos.
d. Evaluación continua de vulnerabilidades y remediación.
e. Uso controlado de privilegios administrativos.
f. Mantenimiento, monitorización y análisis de trazas de auditoría.
g. Protecciones de correo electrónico y navegadores web.
h. Defensas antimalware.
i. Control de puertos de red, protocolos y servicios.
j. Capacidad de recuperación de datos y copias de seguridad.
k. Configuraciones seguras para dispositivos de red como cortafuegos, enrutadores y switches.
l. Acceso controlado basado en la necesidad de conocer.
m. Control de acceso inalámbrico.
n. Control y monitorización de cuentas de usuario.
o. Seguridad del software.
p. Respuesta ante incidentes
q. Pruebas de penetración.

Día 2: Auditoría Interna de ciberseguridad.
Nos conectamos a tu sistema con uno de tus PC y los permisos de un empleado corriente, y verificamos la permeabilidad de la red y la posibilidad de movernos lateralmente accediendo a sistemas e información a la que no deberíamos de tener acceso.

Día 3: Auditoría Externa de intrusión.
Desde nuestras oficinas revisamos las vulnerabilidades de tu infraestructura publicada en Internet (WEB, FTP, VPN, etc.) en base a la metodología OWASP, con el objetivo de tratar de penetrar en tus sistemas.

Día 4: Análisis de exposición digital.
Analizamos la huella pública que la compañía tiene en Internet, recopilando fugas de información, datos expuestos, campañas de desinformación y demás datos que puedan desestabilizar a la organización.

Día 5: Plan de acción
Emitimos un informe final con un plan de acción priorizado, en el que se listarán los trabajos a realizar para poner solución a los problemas identificados.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE